THIRD POWER OF THE REVERSED DICKSON POLYNOMIAL OVER FINITE FIELDS

XIANG-DONG HOU

ABSTRACT. Let $D_n(1,x)$ be the nth reversed Dickson polynomial. The power sums $\sum_{a \in \mathbb{F}_q} D_n(1,a)^i$, $i = 1, 2$, have been determined recently. In this paper we give an evaluation of the sum $\sum_{a \in \mathbb{F}_q} D_n(1,a)^3$. This result implies new necessary conditions for $D_n(1,x)$ to be a permutation polynomial over $\mathbb{F}_q$.

1. INTRODUCTION

Let $n \geq 0$ be an integer and let $\mathbb{F}_q$ denote the finite field with q elements. The nth *reversed Dickson polynomial* $D_n(1,x) \in \mathbb{Z}[x]$ is defined by the functional equation

$$D_n(1, x(1-x)) = x^n + (1-x)^n.$$

Naturally, $D_n(1,x)$ can be viewed as a polynomial over $\mathbb{F}_q$. The reversed Dickson polynomial is a descendant of the polynomial $D_n(x,y) \in \mathbb{Z}[x,y]$ defined by the functional equation

$$D_n(x+y, xy) = x^n + y^n.$$

The other descendant of $D_n(x,y)$ is the well known *Dickson polynomial* $D_n(x,a) \in \mathbb{F}_q[x]$ where $a \in \mathbb{F}_q$. While Dickson polynomials have been the focus of many researchers for over a century (cf. [5]), the significance of reversed Dickson polynomials over finite fields was not clear until some ten years ago. In [1], Dillon explored a connection between reversed Dickson polynomials that are permutations of $\mathbb{F}_{2^m}$ and *almost perfect nonlinear* (APN) functions over $\mathbb{F}_{2^m}$. A more comprehensive approach to reversed Dickson polynomials as permutation polynomials over finite fields appeared in a recent paper [4]. We are interested in the pairs (q,n) for which $D_n(1,x)$ is a permutation polynomial over $\mathbb{F}_q$ and we call such pairs *desirable* [2]. As explained in the introduction of [3], when searching for desirable pairs (q,n), we may assume $1 \leq n \leq q^2 - 2$. All known families (ten families) of desirable pairs are listed in Table 1 of [3]. Computer search has confirmed that there are no other desirable pairs for $q \leq 401$. So the big open question is whether the list of known desirable pairs is complete. Any new addition to the list would be extremely interesting since most families in the list are already highly nontrivial. Another way to attack the problem is to find new necessary conditions for a pair to be desirable. It is well known that a function $f : \mathbb{F}_q \to \mathbb{F}_q$ is bijective if and only if

$$\sum_{a \in \mathbb{F}_q} f(a)^i \begin{cases} = 0 & \text{if } 1 \leq i \leq q-2, \\ \neq 0 & \text{if } i = q-1. \end{cases}$$

Therefore, an explicit evaluation of the sum $\sum_{a \in \mathbb{F}_q} D_n(1,a)^i$ for any $1 \leq i \leq q-1$ would provide necessary conditions for (q,n) to be desirable. The sums

---

$\sum_{a \in \mathbb{F}_q} D_n(1, a)^i$, $i = 1, 2$, have been determined in [3] for this purpose. In the present paper, we give an explicit evaluation of the sum $\sum_{a \in \mathbb{F}_q} D_n(1, a)^3$. As expected, this result implies new necessary conditions for (q, n) to be desirable.

In Section 2 we recall certain results from [3] to be used in the present paper. The evaluation of the sum $\sum_{a \in \mathbb{F}_q} D_n(1, a)^3$ requires separate treatments of the even q case and the odd q case. These two cases are covered in Sections 3 and 4 respectively.

2. PRELIMINARIES

We first prove a lemma

Lemma 2.1. *Let* $q = p^e$, *where* p *is a prime and* $e > 0$. *Let* $0 \leq \alpha, v \leq q - 1$. *Then in* $\mathbb{F}_p$,

$$\binom{q - 1 + \alpha - v}{\alpha} = (-1)^\alpha \binom{v}{\alpha}.$$

Proof. Write $\alpha = \sum_{i=0}^{e-1} \alpha_i p^i$, $v = \sum_{i=0}^{e-1} v_i p^i$, $0 \leq \alpha_i, v_i \leq p - 1$. If $v_i < \alpha_i$ for some i, then $\binom{v}{\alpha} = 0$ and $\binom{q-1+\alpha-v}{\alpha} = 0$. (The second equation holds since the sum $\alpha + (q - 1 - v)$ has carry in base p.) Now assume $v_i \geq \alpha_i$ for all $0 \leq i \leq e - 1$. Then

$$\binom{q - 1 + \alpha - v}{\alpha} = \prod_{i=0}^{e-1} \binom{p - 1 + \alpha_i - v_i}{\alpha_i} = \prod_{i=0}^{e-1} (-1)^{\alpha_i} \binom{v_i}{\alpha_i} = (-1)^\alpha \binom{v}{\alpha}.$$

$\square$

Let $d_n = D_n(1, x)$. Since

$$
\begin{aligned}
d_n(x(1 - x))^3 &= \big[x^n + (1 - x)^n \big]^3 \\
&= x^{3n} + (1 - x)^{3n} + 3 \big[x(1 - x) \big]^n \big[x^n + (1 - x)^n \big] \\
&= d_{3n}(x(1 - x)) + 3 \big[x(1 - x) \big]^n d_n(x(1 - x)),
\end{aligned}
$$

we have

$$(2.1) \qquad\qquad d_n^3 = d_{3n} + 3x^n d_n.$$

Therefore

$$(2.2) \qquad\qquad \sum_{a \in \mathbb{F}_q} d_n(a)^3 = \sum_{a \in \mathbb{F}_q} d_{3n}(a) + 3 \sum_{a \in \mathbb{F}_q} a^n d_n(a).$$

In (2.2), the sum $\sum_{a \in \mathbb{F}_q} d_{3n}(a)$ has been determined in [3]; the goal of the present paper is to evaluate the sum $\sum_{a \in \mathbb{F}_q} a^n d_n(a)$.

By (4.3) of [3],

$$(2.3) \qquad \sum_{n=1}^{q^2-1} d_n t^n \equiv \frac{t(t^{q^2-1} - 1)}{t - 1} + h(t) \sum_{k=1}^{q-1} (t - 1)^{q-1-k} t^{2k} x^k \pmod{x^q - x},$$

where

$$(2.4) \qquad h(t) = \frac{(t - 2)(t^{q^2-1} - 1)}{(t^{q-1} - 1)(t^q - t^{q-1} - 1)} \in \mathbb{F}_p[t] \qquad (p = \operatorname{char} \mathbb{F}_q).$$

Summing both sides of (2.3) as x runs over $\mathbb{F}_q$, we get

$$(2.5) \qquad \sum_{n=2(q-1)}^{q^2-1} \left(\sum_{a \in \mathbb{F}_q} d_n(a) \right) t^n = -t^{2(q-1)} h(t).$$

Lemma 2.2 ([3, Proposition 4.1]). *Assume that q is even. Then*

$$(2.6) \qquad h(t) = \sum_{\substack{\alpha,\beta \geq 0 \\ \alpha+\beta \leq q-2}} \binom{\alpha+\beta}{\alpha} t^{(q-1)^2 - (\alpha+\beta q)}.$$

Lemma 2.3. *Assume that q is odd. Then*
$$(2.7)$$
$$h(t) = t^{(q-1)^2} + \sum_{\substack{\alpha,\beta \geq 0 \\ \beta \leq q-2 \\ 0 < \alpha+\beta \leq q-1}} \left[2^{\alpha+\beta} \binom{2(q-1)-\alpha-\beta}{q-1} - \binom{\alpha+\beta}{\alpha} \right] t^{(q-1)^2 - (\alpha+\beta q)}.$$

Proof. Let $f_n(x) = \sum_{j \geq 0} \binom{n}{2j} x^j$. Let $n = \alpha + \beta q$, where $0 \leq \alpha, \beta \leq q-1$. When $1 \leq n \leq q^2 - 2$, we have

$$\sum_{a \in \mathbb{F}_q} d_n(a)$$

$$= \left(\frac{1}{2} \right)^{n-1} \sum_{a \in \mathbb{F}_q} f_n(a) \qquad \text{(by [3, Proposition 2.1])}$$

$$= \left(\frac{1}{2} \right)^{n-1} \left(-\frac{1}{2} \right) \left[\binom{\alpha+\beta}{q-1} - 2^{\alpha+\beta} \binom{2(q-1)-\alpha-\beta}{q-1-\alpha} \right] \qquad \text{(by [3, Theorem 3.1])}$$

$$= -2^{-\alpha-\beta} \binom{\alpha+\beta}{q-1} + \binom{2(q-1)-\alpha-\beta}{q-1-\alpha}.$$

When $n = q^2 - 1$, since $d_{q^2-1}(x) \equiv x^{q-1} + 1 \pmod{x^q - x}$, we have

$$\sum_{a \in \mathbb{F}_q} d_{q^2-1}(a) = -1.$$

To sum up, we have

$$(2.8) \quad \sum_{a \in \mathbb{F}_q} d_n(a) = \begin{cases} -2^{-\alpha-\beta} \dbinom{\alpha+\beta}{q-1} + \dbinom{2(q-1)-\alpha-\beta}{q-1-\alpha} & \text{if } 1 \leq n \leq q^2 - 2, \\ \\ -1 & \text{if } n = q^2 - 1. \end{cases}$$

Therefore,

$$h(t)$$

$$= -\sum_{n=2(q-1)}^{q^2-1} \Big(\sum_{a\in\mathbb{F}_q} d_n(a)\Big) t^{n-2(q-1)} \qquad\qquad \text{(by (2.5))}$$

$$= -\sum_{i=0}^{(q-1)^2} \Big(\sum_{a\in\mathbb{F}_q} d_{q^2-1-i}(a)\Big) t^{(q-1)^2-i} \qquad\qquad (n=q^2-1-i)$$

$$= t^{(q-1)^2} + \sum_{\substack{0\le\alpha,\beta\le q-1 \\ 0<\alpha+\beta q\le (q-1)^2}} \Big[2^{\alpha+\beta}\binom{2(q-1)-\alpha-\beta}{q-1} - \binom{\alpha+\beta}{\alpha}\Big] t^{(q-1)^2-(\alpha+\beta q)}$$

$$\qquad\qquad\qquad\qquad\qquad (i=\alpha+\beta q \text{ and by (2.8)}).$$

In the above sum, if $\alpha+\beta\ge q$, then $\binom{2(q-1)-\alpha-\beta}{q-1}=0$ and $\binom{\alpha+\beta}{\alpha}=0$. (The second equation holds since the sum $\alpha+\beta$ has carry in base p.) Therefore (2.7) follows. $\square$

In (2.3) substitute t by xt. We then have

$$\sum_{n=1}^{q^2-1} d_n x^n t^n$$

$$\equiv \frac{xt[(xt)^{q^2-1}-1]}{xt-1} + h(xt)\sum_{k=1}^{q-1}(xt-1)^{q-1-k}(xt)^{2k}x^k \pmod{x^q-x}$$

$$\equiv \frac{xt(1-t^{q^2-1})}{1-xt} + h(xt)\sum_{k=1}^{q-1}(xt-1)^{q-1-k}t^{2k}x^{3k} \pmod{x^q-x}.$$

Since

$$\frac{1}{1-xt} = \sum_{k\ge 0} x^k t^k$$

$$= 1 + \sum_{k=1}^{q-1}\sum_{l\ge 0} x^{k+l(q-1)}t^{k+l(q-1)}$$

$$\equiv 1 + \sum_{k=1}^{q-1} x^k t^k \sum_{l\ge 0} t^{l(q-1)} \pmod{x^q-x}$$

$$= 1 + \frac{1}{1-t^{q-1}}\sum_{k=1}^{q-1} x^k t^k,$$

we have

(2.9)

$$\sum_{n=1}^{q^2-1} d_n x^n t^n$$

$$\equiv xt(1-t^{q^2-1})\left[1+\frac{1}{1-t^{q-1}}\sum_{k=1}^{q-1}x^k t^k\right]+h(xt)\sum_{k=1}^{q-1}(xt-1)^{q-1-k}t^{2k}x^{3k} \pmod{x^q-x}$$

$$= (t-t^{q^2})x+\frac{t^{q^2-1}-1}{t^{q-1}-1}\sum_{k=1}^{q-1}t^{k+1}x^{k+1}+h(xt)\sum_{k=1}^{q-1}(xt-1)^{q-1-k}t^{2k}x^{3k}.$$

From here on, the even q case and the odd q case have to be considered separately.

3. THE EVEN q CASE

Assume that q is even. By Lemma 2.2,

(3.1)

$$h(xt) = \sum_{\substack{\alpha,\beta\geq 0 \\ \alpha+\beta\leq q-2}} \binom{\alpha+\beta}{\alpha}t^{(q-1)^2-(\alpha+\beta q)}x^{(q-1)^2-(\alpha+\beta q)}$$

$$\equiv \sum_{\substack{\alpha,\beta\geq 0 \\ \alpha+\beta\leq q-2}} \binom{\alpha+\beta}{\alpha}t^{(q-1)^2-(\alpha+\beta q)}x^{q-1-(\alpha+\beta)} \pmod{x^q-x}.$$

By (2.9) and (3.1),

$$\sum_{n=1}^{q^2-1} d_n x^n t^n$$

$$\equiv (t-t^{q^2})x+\frac{t^{q^2-1}-1}{t^{q-1}-1}\sum_{k=1}^{q-1}t^{k+1}x^{k+1}$$

$$+\sum_{\substack{\alpha,\beta\geq 0 \\ \alpha+\beta\leq q-2}}\sum_{k=1}^{q-1}\binom{\alpha+\beta}{\alpha}(xt-1)^{q-1-k}t^{(q-1)^2+2k-(\alpha+\beta q)}x^{q-1+3k-(\alpha+\beta)}$$

$$\pmod{x^q-x}$$

$$= (t-t^{q^2})x+\frac{t^{q^2-1}-1}{t^{q-1}-1}\sum_{k=1}^{q-1}t^{k+1}x^{k+1}$$

$$+\sum_{\substack{\alpha,\beta\geq 0 \\ \alpha+\beta\leq q-2}}\sum_{k=1}^{q-1}\sum_{j}\binom{\alpha+\beta}{\alpha}\binom{q-1-k}{j}(xt)^{q-1-k-j}t^{(q-1)^2+2k-(\alpha+\beta q)}x^{q-1+3k-(\alpha+\beta)}$$

$$= (t-t^{q^2})x+\frac{t^{q^2-1}-1}{t^{q-1}-1}\sum_{k=1}^{q-1}t^{k+1}x^{k+1}$$

$$+\sum_{\substack{\alpha,\beta\geq 0 \\ \alpha+\beta\leq q-2}}\sum_{k=1}^{q-1}\sum_{j}\binom{\alpha+\beta}{\alpha}\binom{q-1-k}{j}t^{q(q-1)+k-j-(\alpha+\beta q)}x^{2(q-1)+2k-j-(\alpha+\beta)}.$$

Let x vary over $\mathbb{F}_q$ and sum both sides of the above equation. We get

$$\sum_{n=1}^{q^2-1}\Big(\sum_{a\in\mathbb{F}_q}a^n d_n(a)\Big)t^n$$

$$=\frac{t^{q^2-1}-1}{t^{q-1}-1}t^{q-1}+\sum_{\substack{\alpha,\beta,j\geq 0;k\geq 1\\ \alpha+\beta\leq q-2;j+k\leq q-1\\ 2k-j-(\alpha+\beta)\equiv 0\ (\mathrm{mod}\ q-1)}}\binom{\alpha+\beta}{\alpha}\binom{q-1-k}{j}t^{q(q-1)+k-j-(\alpha+\beta q)}$$

$$=\sum_{l=1}^{q+1}t^{l(q-1)}+\sum_{\substack{\alpha,\beta,j\geq 0;k\geq 1\\ \alpha+\beta\leq q-2;j+k\leq q-1\\ 2k-j-(\alpha+\beta)\equiv 0\ (\mathrm{mod}\ q-1)}}\binom{\alpha+\beta}{\alpha}\binom{q-1-k}{j}t^{q(q-1)+k-j-(\alpha+\beta q)}.$$

Therefore, for $1\leq n\leq q^2-1$,

$$(3.2)\qquad \sum_{a\in\mathbb{F}_q}a^n d_n(a)=\delta_n+\sum_{\substack{\alpha,\beta,j\geq 0;k\geq 1\\ \alpha+\beta\leq q-2;j+k\leq q-1\\ 2k-j-(\alpha+\beta)\equiv 0\ (\mathrm{mod}\ q-1)\\ q(q-1)+k-j-(\alpha+\beta q)=n}}\binom{\alpha+\beta}{\alpha}\binom{q-1-k}{j},$$

where

$$(3.3)\qquad \delta_n=\begin{cases}1 & \text{if } n\equiv 0\pmod{q-1},\\ 0 & \text{if } n\not\equiv 0\pmod{q-1}.\end{cases}$$

Proposition 3.1. *Let q be a power of 2. Let $1\leq n\leq q^2-1$ and write $n=u+vq$, $0\leq u,v\leq q-1$. Then in $\mathbb{F}_2$,*

$$(3.4)$$

$$\sum_{a\in\mathbb{F}_q}a^n d_n(a)$$

$$=\delta_n+\sum_{-1\leq s\leq 2}\ \sum_{\max\{s-\frac{u+v}{q-1},v-q+1\}\leq\epsilon<\min\{s-\frac{u+v}{q-1}+1,v\}}\binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon}.$$

Proof. First note that in the sum on the right side of (3.2), the condition $q(q-1)+k-j-(\alpha+\beta q)=n$ is equivalent to $k-j-\alpha-u+(q-1-\beta-v)q$, which is further equivalent to

$$\begin{cases}k-j-\alpha-u=\epsilon q,\\ q-1-\beta-v+\epsilon=0\end{cases}$$

for some $\epsilon\in\mathbb{Z}$. Therefore, the conditions on α,β,j,k in that sum can be *replaced* by

$$(3.5)\qquad \begin{cases}\beta\geq 0,\\ 1\leq k\leq q-1,\\ 0\leq\alpha\leq q-2-\beta,\\ 2k-j-(\alpha+\beta)=s(q-1),\quad -1\leq s\leq 2,\\ k-j-\alpha-u=\epsilon q,\quad \epsilon\in\mathbb{Z},\\ q-1-\beta-v+\epsilon=0.\end{cases}$$

(Note. We remind the reader that (3.5) is not equivalent to but weaker than the conditions in the sum in (3.2); the restriction on j is not present in (3.5). However, the relaxation only brings additional zero terms to the sum in (3.2).) We solve (3.5) for β, k, j in terms of α, s, ϵ. The result is

(3.6)
$$\begin{cases} \beta = q - 1 + \epsilon - v, \\ k = (s - \epsilon + 1)(q-1) - u - v, \\ j = (s - 2\epsilon + 1)(q-1) - 2u - v - \alpha - \epsilon, \\ -1 \leq s \leq 2, \\ \dfrac{u+v}{q-1} - 1 < s - \epsilon \leq \dfrac{u+v}{q-1}, \\ \epsilon \geq v - q + 1, \\ 0 \leq \alpha \leq v - 1 - \epsilon. \end{cases}$$

Now (3.2) can be written as

(3.7)
$$\delta_n + \sum_{a \in \mathbb{F}-q} a^n d_n(a)$$

$$= \sum_{\substack{s,\epsilon \\ -1 \leq s \leq 2 \\ \frac{u+v}{q-1}-1<s-\epsilon\leq\frac{u+v}{q-1}, \\ \epsilon \geq v-q+1}} \sum_{0 \leq \alpha \leq v-1-\epsilon} \binom{\alpha + q - 1 + \epsilon - v}{\alpha} \binom{u + v - (s-\epsilon)(q-1)}{(s - 2\epsilon + 1)(q-1) - 2u - v - \alpha - \epsilon}$$

$$= \sum_{\substack{s,\epsilon \\ -1 \leq s \leq 2 \\ \frac{u+v}{q-1}-1<s-\epsilon\leq\frac{u+v}{q-1}, \\ v-q+1\leq\epsilon\leq v-1}} \sum_{0 \leq \alpha \leq v-1-\epsilon} \binom{q - 1 + \alpha - (v - \epsilon)}{\alpha} \binom{u + v - (s-\epsilon)(q-1)}{(s - 2\epsilon + 1)(q-1) - 2u - v - \epsilon - \alpha}$$

$$= \sum_{\substack{s,\epsilon \\ -1 \leq s \leq 2 \\ \frac{u+v}{q-1}-1<s-\epsilon\leq\frac{u+v}{q-1}, \\ v-q+1\leq\epsilon\leq v-1}} \sum_{0 \leq \alpha \leq v-1-\epsilon} \binom{v - \epsilon}{\alpha} \binom{u + v - (s-\epsilon)(q-1)}{(s - 2\epsilon + 1)(q-1) - 2u - v - \epsilon - \alpha}$$

(by Lemma 2.1)

$$= \sum_{\substack{s,\epsilon \\ -1 \leq s \leq 2 \\ \frac{u+v}{q-1}-1<s-\epsilon\leq\frac{u+v}{q-1}, \\ v-q+1\leq\epsilon\leq v-1}} \left[\binom{u + v - (s-\epsilon)(q-1)}{(s - 2\epsilon + 1)(q-1) - 2u - 2v} \right.$$

$$\left. + \sum_{0 \leq \alpha \leq v-\epsilon} \binom{v - \epsilon}{\alpha} \binom{u + v - (s-\epsilon)(q-1)}{(s - 2\epsilon + 1)(q-1) - 2u - v - \epsilon - \alpha} \right]$$

$$= \sum_{\substack{s,\epsilon \\ -1 \leq s \leq 2 \\ \frac{u+v}{q-1}-1<s-\epsilon\leq\frac{u+v}{q-1}, \\ v-q+1\leq\epsilon\leq v-1}} \left[\binom{u + v - (s-\epsilon)(q-1)}{(s - 2\epsilon + 1)(q-1) - 2u - 2v} + \binom{u + v - (s-\epsilon)(q-1) + v - \epsilon}{(s - 2\epsilon + 1)(q-1) - 2u - 2v + v - \epsilon} \right]$$

$$= \sum_{\substack{s,\epsilon \\ -1 \le s \le 2 \\ \frac{u+v}{q-1}-1 < s-\epsilon \le \frac{u+v}{q-1}, \\ v-q+1 \le \epsilon \le v-1}} \binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-2v+v-\epsilon}$$

$$= \sum_{-1 \le s \le 2} \sum_{\max\{s-\frac{u+v}{q-1},v-q+1\} \le \epsilon < \min\{s-\frac{u+v}{q-1}+1,v\}} \binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon}.$$

$\square$

Note. In (3.4), for each $-1 \le s \le 2$, there is at most one ϵ in the specified range. Thus the sum in (3.4) contains at most four terms. More precisely, (3.4) can be stated as follows.

When $0 < u+v < q-1$,

(3.8)
$$\sum_{a \in \mathbb{F}_q} a^n d_n(a) = \sum_{-1 \le s \le \min\{2,v-1\}} \binom{u+v}{(-s+1)(q-1)-2u-v-s}$$

$$= \sum_{-1 \le s \le \min\{0,v-1\}} \binom{u+v}{(-s+1)(q-1)-2u-v-s}$$

$$= \begin{cases} \binom{u}{2(q-1)-2u+1} & \text{if } v=0, \\ \binom{u+v}{2(q-1)-2u-v+1} + \binom{u+v}{q-1-2u-v} & \text{if } v>0. \end{cases}$$

When $q-1 \le u+v < 2(q-1)$,

(3.9)
$$\sum_{a \in \mathbb{F}_q} a^n d_n(a) = \delta_n + \sum_{\max\{-1,v-q+2\} \le s \le \min\{2,v\}} \binom{u+v-(q-1)}{(-s+3)(q-1)-2u-v-s+1}$$

$$= \delta_n + \sum_{\max\{0,v-q+2\} \le s \le \min\{1,v\}} \binom{u+v-(q-1)}{(-s+3)(q-1)-2u-v-s+1}$$

$$= \begin{cases} 1 & \text{if } v=0, \\ \delta_n + \binom{u+v-(q-1)}{3(q-1)-2u-v+1} + \binom{u+v-(q-1)}{2(q-1)-2u-v} & \text{if } 1 \le v \le q-2, \\ \delta_n + \binom{u}{q-1-2u} & \text{if } v=q-1. \end{cases}$$

Theorem 3.2. *Let q be a power of 2 and let $1 \leq n \leq q^2 - 1$ Write $n = u + vq$, $0 \leq u, v \leq q - 1$, and write $3n \equiv u' + v'q \pmod{q^2 - 1}$, $0 \leq u', v' \leq q - 1$. Then*

(3.10)
$$\sum_{a \in \mathbb{F}_q} d_n(a)^3$$

$$= \delta_n + \sum_{-1 \leq s \leq 2} \sum_{\max\{s - \frac{u+v}{q-1}, v-q+1\} \leq \epsilon < \min\{s - \frac{u+v}{q-1} + 1, v\}} \binom{u + v - (s - \epsilon)(q - 1)}{(s - 2\epsilon + 1)(q - 1) - 2u - v - \epsilon}$$

$$+ \begin{cases} \binom{2(q-1) - u' - v'}{q - 1 - u'} & \text{if } u' + v' \geq q, \\ 0 & \text{if } u' + v' < q. \end{cases}$$

Proof. By (2.2),
$$\sum_{a \in \mathbb{F}_q} d_n(a)^3 = \sum_{a \in \mathbb{F}_q} a^n d_n(a) + \sum_{a \in \mathbb{F}_q} d_{3n}(a).$$

In the above, $\sum_{a \in \mathbb{F}_q} a^n d_n(a)$ is given by (3.4). By [3, Theorem 4.2],

(3.11)
$$\sum_{a \in \mathbb{F}_q} d_{3n}(a) = \begin{cases} \binom{2(q-1) - u' - v'}{q - 1 - u'} & \text{if } u' + v' \geq q, \\ 0 & \text{if } u' + v' < q. \end{cases}$$

□

Corollary 3.3. *In Theorem 3.2 assume $q > 4$ and (q, n) is desirable. Then $0 < u + v < q - 1$ or $q - 1 < u + v < 2(q - 1)$.*

(i) *If $0 < u + v < q - 1$, then in $\mathbb{F}_2$,*

(3.12)
$$\sum_{-1 \leq s \leq \min\{0, v-1\}} \binom{u + v}{(-s + 1)(q - 1) - 2u - v - s}$$
$$= \begin{cases} \binom{2(q-1) - u' - v'}{q - 1 - u'} & \text{if } u' + v' \geq q, \\ 0 & \text{if } u' + v' < q. \end{cases}$$

(ii) *If $q - 1 < u + v < 2(q - 1)$, then in $\mathbb{F}_2$,*

(3.13)
$$\sum_{\max\{0, v-q+2\} \leq s \leq \min\{1, v\}} \binom{u + v - (q - 1)}{(-s + 3)(q - 1) - 2u - v - s + 1}$$
$$= \begin{cases} \binom{2(q-1) - u' - v'}{q - 1 - u'} & \text{if } u' + v' \geq q, \\ 0 & \text{if } u' + v' < q. \end{cases}$$

Proof. By [3, Theorem 2.5], $(n, q^2 - 1) = 3 < q - 1$. Thus $u + v \not\equiv 0 \pmod{q - 1}$, namely, $0 < u + v < q - 1$ or $q - 1 < u + v < 2(q - 1)$. Since $\sum_{a \in \mathbb{F}_q} a^n d_n(a) + \sum_{a \in \mathbb{F}_q} d_{3n}(a) = \sum_{a \in \mathbb{F}_q} d_n(a)^3 = 0$, (3.8) and (3.11) yield (3.12); (3.9) and (3.11) yield (3.13). □

4. The Odd q Case

Assume that q is an odd prime power. The plan of this section is parallel to that of Section 3. Starting from the end of Section 2, we proceed to determine the sum $\sum_{a \in \mathbb{F}_q} a^n d_n(a)$.

By Lemma 2.3,

(4.1)
$$h(xt)$$
$$= (xt)^{(q-1)^2}$$
$$+ \sum_{\substack{\alpha,\beta \geq 0; \beta \leq q-2 \\ 0 < \alpha+\beta \leq q-1}} \left[2^{\alpha+\beta} \binom{2(q-1)-\alpha-\beta}{q-1} - \binom{\alpha+\beta}{\alpha} \right] t^{(q-1)^2-(\alpha+\beta q)} x^{(q-1)^2-(\alpha+\beta q)}$$
$$\equiv t^{(q-1)^2} x^{q-1}$$
$$+ \sum_{\substack{\alpha,\beta \geq 0; \beta \leq q-2 \\ 0 < \alpha+\beta \leq q-1}} \left[2^{\alpha+\beta} \binom{2(q-1)-\alpha-\beta}{q-1} - \binom{\alpha+\beta}{\alpha} \right] t^{(q-1)^2-(\alpha+\beta q)} x^{2(q-1)-(\alpha+\beta)}$$
$$\pmod{x^q - x}.$$

By (2.9) and (4.1),

$$\sum_{n=1}^{q^2-1} d_n x^n t^n$$
$$\equiv (t - t^{q^2})x + \frac{t^{q^2-1}-1}{t^{q-1}-1} \sum_{k=1}^{q-1} t^{k+1} x^{k+1}$$
$$+ \left[t^{(q-1)^2} x^{q-1} + \sum_{\substack{\alpha,\beta \geq 0; \beta \leq q-2 \\ 0 < \alpha+\beta \leq q-1}} \left[2^{\alpha+\beta} \binom{2(q-1)-\alpha-\beta}{q-1} - \binom{\alpha+\beta}{\alpha} \right] t^{(q-1)^2-(\alpha+\beta q)} x^{2(q-1)-(\alpha+\beta)} \right]$$
$$\cdot \sum_{\substack{k \geq 1; j \geq 0 \\ k+j \leq q-1}} \binom{q-1-k}{j} (-1)^j (xt)^{q-1-k-j} t^{2k} x^{3k} \qquad \pmod{x^q - x}$$
$$\equiv (t - t^{q^2})x + \frac{t^{q^2-1}-1}{t^{q-1}-1} \sum_{k=1}^{q-1} t^{k+1} x^{k+1}$$
$$+ \sum_{\substack{k \geq 1; j \geq 0 \\ k+j \leq q-1}} \binom{q-1-k}{j} (-1)^j t^{q(q-1)+k-j} x^{q-1+2k-j}$$
$$+ \sum_{\substack{\alpha,\beta \geq 0; \beta \leq q-2 \\ 0 < \alpha+\beta \leq q-1}} \sum_{\substack{k \geq 1; j \geq 0 \\ k+j \leq q-1}} \left[2^{\alpha+\beta} \binom{2(q-1)-\alpha-\beta}{q-1} - \binom{\alpha+\beta}{\alpha} \right]$$
$$\cdot \binom{q-1-k}{j} (-1)^j t^{q(q-1)+k-j-(\alpha+\beta q)} x^{2(q-1)+2k-j-(\alpha+\beta)} \qquad \pmod{x^q - x}.$$

Let x vary over $\mathbb{F}_q$ and sum both sides of the above equation. We have

$$\sum_{n=1}^{q^2-1}\left(\sum_{a\in\mathbb{F}_q}a^n d_n(a)\right)t^n$$

$$= -\frac{t^{q^2-1}-1}{t^{q-1}-1}t^{q-1} - \sum_{\substack{k\geq 1;j\geq 0\\k+j\leq q-1\\2k-j\equiv 0\;(\mathrm{mod}\;q-1)}}\binom{q-1-k}{j}(-1)^j t^{q(q-1)+k-j}$$

$$-\sum_{\substack{\alpha,\beta\geq 0;\beta\leq q-2\\0<\alpha+\beta\leq q-1}}\sum_{\substack{k\geq 1;j\geq 0\\k+j\leq q-1\\2k-j\equiv\alpha+\beta\;(\mathrm{mod}\;q-1)}}\left[2^{\alpha+\beta}\binom{2(q-1)-\alpha-\beta}{q-1}-\binom{\alpha+\beta}{\alpha}\right]$$

$$\cdot\binom{q-1-k}{j}(-1)^j t^{q(q-1)+k-j-(\alpha+\beta q)}.$$

Thus, for $1\leq n\leq q^2-1$,

$$\sum_{a\in\mathbb{F}_q}a^n d_n(a) = -\delta_n - \mathrm{I} - \mathrm{II} + \mathrm{III},$$

where δ_n is defined in (3.3) and

(4.2) $$\mathrm{I} = \sum_{\substack{k\geq 1;j\geq 0\\k+j\leq q-1\\2k-j\equiv 0\;(\mathrm{mod}\;q-1)\\q(q-1)+k-j=n}}\binom{q-1-k}{j}(-1)^j,$$

(4.3)

$$\mathrm{II} = \sum_{\substack{\alpha,\beta\geq 0;\beta\leq q-2\\0<\alpha+\beta\leq q-1}}\sum_{\substack{k\geq 1;j\geq 0\\k+j\leq q-1\\2k-j\equiv\alpha+\beta\;(\mathrm{mod}\;q-1)\\q(q-1)+k-j-(\alpha+\beta q)=n}}2^{\alpha+\beta}\binom{2(q-1)-\alpha-\beta}{q-1}\binom{q-1-k}{j}(-1)^j,$$

(4.4) $$\mathrm{III} = \sum_{\substack{\alpha,\beta\geq 0;\beta\leq q-2\\0<\alpha+\beta\leq q-1}}\sum_{\substack{k\geq 1;j\geq 0\\k+j\leq q-1\\2k-j\equiv\alpha+\beta\;(\mathrm{mod}\;q-1)\\q(q-1)+k-j-(\alpha+\beta q)=n}}\binom{\alpha+\beta}{\alpha}\binom{q-1-k}{j}(-1)^j.$$

We now determine the sums I, II and III separately. Write $n = u + vq$, $0\leq u,v\leq q-1$.

Lemma 4.1. *Assume $1\leq n\leq q^2-2$. We have*

(4.5) $$\mathrm{I} = \sum_{\max\{-1,v-q+\frac{u+v}{q-1}\}<s\leq v-q+\frac{u+v}{q-1}+1}\binom{u+v-(s-v+q-1)(q-1)}{(s-2v+2q)(q-1)-2(u+v)}.$$

Proof. In the sum in (4.2), the conditions on k and j can be *replaced* by

(4.6) $$\begin{cases}0 < k\leq q-1,\\2k-j = s(q-1),\quad 0\leq s\leq 2,\\q(q-1)+k-j = u+vq.\end{cases}$$

(Note. In (4.6) we dropped the restriction on j. However, this relaxation has no effect on the sum in (4.2) since only additional zero terms are brought in.) Solving (4.6) for k and j in terms of s, we get

$$\begin{cases} k = (s - v + q)(q - 1) - u - v, \\ j = (s - 2v + 2q)(q - 1) - 2(u + v), \\ \max\{-1, v - q + \dfrac{u + v}{q - 1}\} < s \le v - q + \dfrac{u + v}{q - 1} + 1. \end{cases}$$

Thus

$$\mathrm{I} = \sum_{\max\{-1, v - q + \frac{u+v}{q-1}\} < s \le v - q + \frac{u+v}{q-1} + 1} \binom{u + v - (s - v + q - 1)(q - 1)}{(s - 2v + 2q)(q - 1) - 2(u + v)}.$$

$\square$

Note. The sum in (4.5) has at most one term. More precisely, when $0 < u + v < q - 1$,

$$(4.7) \qquad\qquad\qquad \mathrm{I} = 0.$$

When $q - 1 \le u + v < 2(q - 1)$,

$$(4.8) \qquad \mathrm{I} = \begin{cases} \binom{u + v - (q - 1)}{(q + 2 - v)(q - 1) - 2(u + v)} & \text{if } q - 2 \le v \le q - 1, \\ 0 & \text{if } v < q - 2. \end{cases}$$

Lemma 4.2. *We have*
$$(4.9)$$
$$\mathrm{II} = \sum_{\substack{0 \le s \le 2 \\ \max\{0, v - s + \frac{u+v}{q-1}\} < \alpha \le \min\{q-1, v - s + \frac{u+v}{q-1} + 1\}}} \binom{u + v - (s + \alpha - v - 1)(q - 1)}{(s + 2\alpha - 2v)(q - 1) - 2(u + v)}.$$

Proof. First note that if $0 < \alpha + \beta < q - 1$, then $\binom{2(q-1) - \alpha - \beta}{q - 1} = 0$ since the sum $(q - 1) + (q - 1 - \alpha - \beta)$ has carry in base p. Thus

$$(4.10)$$
$$\begin{aligned} \mathrm{II} &= \sum_{\substack{\alpha, \beta \ge 0; \beta \le q-2 \\ \alpha + \beta = q - 1}} \sum_{\substack{k \ge 1; j \ge 0 \\ k + j \le q - 1 \\ 2k - j \equiv \alpha + \beta \ (\mathrm{mod}\ q-1) \\ q(q-1) + k - j - (\alpha + \beta q) = n}} (-1)^j \binom{q - 1 - k}{j} \\ &= \sum_{1 \le \alpha \le q-1} \sum_{\substack{k \ge 1; j \ge 0 \\ k + j \le q - 1 \\ 2k - j \equiv 0 \ (\mathrm{mod}\ q-1) \\ k - j + \alpha(q-1) = n}} (-1)^j \binom{q - 1 - k}{j}. \end{aligned}$$

In (4.10), the conditions on α, k, j can be *replaced* by

$$(4.11) \qquad \begin{cases} 0 < \alpha \le q - 1, \\ 0 < k \le q - 1, \\ 2k - j = s(q - 1), \qquad 0 \le s \le 2, \\ k - j + \alpha(q - 1) = u + vq. \end{cases}$$

Solving (4.11) for k and j in terms of s and α, we have

$$\begin{cases} k = (s + \alpha - v)(q - 1) - u - v, \\ j = (s + 2\alpha - 2v)(q - 1) - 2(u + v), \\ 0 \le s \le 2, \\ \max\{0, v - s + \dfrac{u + v}{q - 1}\} < \alpha \le \min\{q - 1, v - s + \dfrac{u + v}{q - 1} + 1\}. \end{cases}$$

Thus

$$\text{II} = \sum_{\substack{0 \le s \le 2 \\ \max\{0, v - s + \frac{u+v}{q-1}\} < \alpha \le \min\{q-1, v-s+\frac{u+v}{q-1}+1\}}} \binom{u + v - (s + \alpha - v - 1)(q - 1)}{(s + 2\alpha - 2v)(q - 1) - 2(u + v)}.$$

$\square$

Note. In (4.9), for each $0 \le s \le 2$, there is at most one α in the specified range. Hence the sum contains at most three terms. More precisely, when $0 < u+v < q-1$,

$$\begin{aligned} \text{II} &= \sum_{0 \le s \le \min\{2, v\}} \binom{u + v}{(-s + 2)(q - 1) - 2(u + v)} \\ &= \sum_{0 \le s \le \min\{1, v\}} \binom{u + v}{(-s + 2)(q - 1) - 2(u + v)} \\ (4.12) \qquad &= \begin{cases} \binom{u}{2(q - 1) - 2u} & \text{if } v = 0, \\ \binom{u + v}{2(q - 1) - 2(u + v)} + \binom{u + v}{q - 1 - 2(u + v)} & \text{if } 1 \le v \le q - 2. \end{cases} \end{aligned}$$

When $u + v = q - 1$,

$$\begin{aligned} (4.13) \qquad \text{II} &= \sum_{\max\{0, v+3-q\} \le s \le \min\{2, v+1\}} \binom{0}{(-s + 2)(q - 1)} \\ &= \begin{cases} 0 & \text{if } v = 0, \\ 1 & \text{if } 1 \le v \le q - 1. \end{cases} \end{aligned}$$

When $q - 1 < u + v < 2(q - 1)$,

$$\begin{aligned} \text{II} &= \sum_{\max\{0, v+3-q\} \le s \le \min\{2, v+1\}} \binom{u + v - (q - 1)}{(-s + 4)(q - 1) - 2(u + v)} \\ &= \sum_{\max\{0, v+3-q\} \le s \le 1} \binom{u + v - (q - 1)}{(-s + 4)(q - 1) - 2(u + v)} \\ (4.14) \qquad &= \begin{cases} \binom{u + v - (q - 1)}{4(q - 1) - 2(u + v)} + \binom{u + v - (q - 1)}{3(q - 1) - 2(u + v)} & \text{if } 1 \le v \le q - 3, \\ \binom{u - 1}{q + 1 - 2u} & \text{if } v = q - 2, \\ 0 & \text{if } v = q - 1. \end{cases} \end{aligned}$$

Lemma 4.3. *We have*

(4.15)

$$\text{III} = \sum_{\substack{-1 \le s \le 1 \\ \max\{s-\frac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s-\frac{u+v}{q-1}+1, v\}}} (-1)^{v+\epsilon} \binom{u+2v-(s-\epsilon)(q-1)-\epsilon}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon}$$

$$- \sum_{\max\{-2, v-q+\frac{u+v}{q-1}\} < s \le \min\{1, v-q+\frac{u+v}{q-1}+1\}} \binom{u+v-(s-v+q-1)(q-1)}{(s-2v+2q)(q-1)-2(u+v)}.$$

Proof. In (4.4), the conditions on α, β, k, j can be *replaced* by

(4.16)
$$\begin{cases} 0 \le \beta \le q-2, \\ 0 < \alpha + \beta \le q-1, \\ 0 < k \le q-1, \\ 2k-j-(\alpha+\beta) = s(q-1), & -1 \le s \le 1, \\ k-j-\alpha-u = \epsilon q, & \epsilon \in \mathbb{Z}, \\ q-1-\beta-v+\epsilon = 0. \end{cases}$$

Solving (4.16) for k, j, β in terms of α, s, ϵ, we have

$$\begin{cases} \beta = q-1-v+\epsilon, \\ k = (s-\epsilon+1)(q-1)-u-v, \\ j = (s-2\epsilon+1)(q-1)-2u-v-\epsilon-\alpha, \\ -1 \le s \le 1, \\ \max\{s-\dfrac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s-\dfrac{u+v}{q-1}+1, v\}, \\ v-\epsilon-q+1 < \alpha \le v-\epsilon. \end{cases}$$

Therefore,

(4.17)
$$\text{III} = \sum_{\substack{-1 \le s \le 1 \\ \max\{s - \frac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s - \frac{u+v}{q-1}+1, v\}}} \sum_{v-\epsilon-q+1 < \alpha \le v-\epsilon} (-1)^{v+\epsilon+\alpha} \binom{\alpha+q-1-v+\epsilon}{\alpha} \binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon-\alpha}$$

$$= \sum_{\substack{-1 \le s \le 1 \\ \max\{s - \frac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s - \frac{u+v}{q-1}+1, v\}}} \sum_{v-\epsilon-q+1 < \alpha \le v-\epsilon} (-1)^{v+\epsilon} \binom{v-\epsilon}{\alpha} \binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon-\alpha}$$

$$\text{(by Lemma 2.1)}$$

$$= \sum_{\substack{-1 \le s \le 1 \\ \max\{s - \frac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s - \frac{u+v}{q-1}+1, v\}}} (-1)^{v+\epsilon} \Bigg[\binom{u+2v-(s-\epsilon)(q-1)-\epsilon}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon}$$

$$- \sum_{0 \le \alpha \le v-\epsilon-q+1} \binom{v-\epsilon}{\alpha} \binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon-\alpha} \Bigg]$$

$$= \sum_{\substack{-1 \le s \le 1 \\ \max\{s - \frac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s - \frac{u+v}{q-1}+1, v\}}} (-1)^{v+\epsilon} \binom{u+2v-(s-\epsilon)(q-1)-\epsilon}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon} - A,$$

where

(4.18)
$$A = \sum_{\substack{-1 \le s \le 1 \\ \max\{s - \frac{u+v}{q-1}, v-q+1\} \le \epsilon < \min\{s - \frac{u+v}{q-1}+1, v\}}} (-1)^{v+\epsilon}$$

$$\cdot \sum_{0 \le \alpha \le v-\epsilon-q+1} \binom{v-\epsilon}{\alpha} \binom{u+v-(s-\epsilon)(q-1)}{(s-2\epsilon+1)(q-1)-2u-v-\epsilon-\alpha}.$$

Note that in (4.18), $v - q + 1 \le \epsilon$ in the outer sum; thus the inner sum is empty unless $\epsilon = v - q + 1$. Therefore
(4.19)
$$A = \sum_{\max\{-2, v-q+\frac{u+v}{q-1}\} < s \le \min\{1, v-q+\frac{u+v}{q-1}+1\}} \binom{u+v-(s-v+q-1)(q-1)}{(s-2v+2q)(q-1)-2(u+v)}.$$

Equation (4.15) follows from (4.17) and (4.19). □

Note. In (4.15), the first sum has at most three terms and the second sum has at most one term. The formula for III can be made more explicit as we saw earlier in

similar situations. We assume that $q > 3$. When $0 < u + v < q - 1$,

(4.20)

$$
\text{III} = \sum_{-1 \leq s \leq \min\{0, v-1\}} (-1)^{v+s} \binom{u + 2v - s}{(-s+1)(q-1) - 2u - v - s}
$$

$$
= \begin{cases}
-\binom{u+1}{2(q-1) - 2u + 1} & \text{if } v = 0, \\[2mm]
(-1)^{v+1} \binom{u + 2v + 1}{2(q-1) - 2u - v + 1} + (-1)^v \binom{u + 2v}{q - 1 - 2u - v} & \text{if } 1 \leq v \leq q - 2.
\end{cases}
$$

When $q - 1 \leq u + v < 2(q - 1)$,

(4.21)

$$
\text{III} = \sum_{\max\{-1, v-q+2\} \leq s \leq \min\{1, v\}} (-1)^{v+s+1} \binom{u + 2v - q - s + 2}{(-s+3)(q-1) - 2u - v - s + 1}
$$

$$
- \sum_{\max\{-1, v-q+2\} \leq s \leq v-q+2} \binom{u + v - (s - v + q - 1)(q - 1)}{(s - 2v + 2q)(q - 1) - 2(u + v)}
$$

$$
= \begin{cases}
0 & \text{if } v = 0, \\[2mm]
(-1)^v \binom{u + 2v - q + 3}{4(q-1) - 2u - v + 2} + (-1)^{v+1} \binom{u + 2v - q + 2}{3(q-1) - 2u - v + 1} & \\[2mm]
\quad + (-1)^v \binom{u + 2v - q + 1}{2(q-1) - 2u - v} & \text{if } 1 \leq v \leq q - 3, \\[2mm]
\binom{u + q - 2}{2q - 2u} - \binom{u + q - 3}{q - 2u} - \binom{u - 1}{2q - 2u} & \text{if } v = q - 2, \\[2mm]
\binom{u + q - 1}{q - 2u - 1} - \binom{u}{q - 2u - 1} & \text{if } v = q - 1.
\end{cases}
$$

To recap, we have the following proposition.

Proposition 4.4. *Let q be an odd prime power and let $1 \leq n \leq q^2 - 2$. Then*

(4.22)
$$
\sum_{a \in \mathbb{F}_q} a^n d_n(a) = -\delta_n - \text{I} - \text{II} + \text{III},
$$

where δ_n defined in (3.3); I, II, III are given by (4.5), (4.9) and (4.15) respectively.

Theorem 4.5. *Let q be an odd prime power and let $1 \leq n \leq q^2 - 2$. Write $n = u + vq$, $0 \leq u, v \leq q - 1$, and write $3n \equiv u' + v'q > 0 \pmod{q^2 - 1}$, $0 \leq u'v' \leq q - 1$. Then*

(4.23)
$$
\sum_{a \in \mathbb{F}_q} d_n(a)^3 = 3(-\delta_n - \text{I} - \text{II} + \text{III})
$$

$$
+ \begin{cases}
-2^{-u'-v'} \binom{u' + v'}{q - 1} + \binom{2(q-1) - u' - v'}{q - 1 - u'} & \text{if } 1 \leq u' + v'q \leq q^2 - 2, \\[2mm]
-1 & \text{if } u' + v'q = q^2 - 1.
\end{cases}
$$

Proof. This follows from (2.2), (4.22) and (2.8). $\qquad\square$

Corollary 4.6. *In Theorem 4.5 assume $q > 3$ and (q, n) is desirable. Then $u+v \neq q-1$ and in $\mathbb{F}_p$,*

(4.24)
$$
3(\mathrm{I+II-III}) = \begin{cases} -2^{-u'-v'} \dbinom{u' + v'}{q - 1} + \dbinom{2(q - 1) - u' - v'}{q - 1 - u'} & \text{if } 1 \leq u' + v'q \leq q^2 - 2, \\ \\ -1 & \text{if } u' + v'q = q^2 - 1. \end{cases}
$$

Proof. By Theorems 2.3 and 2.4 of [3], $(n, q - 1) \leq 3 < q - 1$. Thus $u + v \neq q - 1$. Now (4.24) follows from (4.23). $\qquad\square$

References

[1] J. F. Dillon, *Geometry, codes and difference sets: exceptional connections*, Codes and Designs (Columbus, OH, 2000), 73 – 85, Ohio State Univ. Math. Res. Inst. Publ., 10, de Gruyter, Berlin, 2002.

[2] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory Ser. A, **118** (2011), 448 – 454.

[3] X. Hou and T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl., **16** (2010), 436 – 448.

[4] X. Hou, G. L. Mullen, J. A. Sellers, J. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. **15** (2009) 748 – 773.

[5] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, Longman Scientific and Technical, Essex, United Kingdom, 1993.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF SOUTH FLORIDA, TAMPA, FL 33620

E-mail address: `xhou@cas.usf.edu`